ABSTRACT

For signing of data by a given one of M delegates mandated by N titleholders, where $M \geq 2$ and $N = 1$ or $M = 1$ and $N \geq 2$, the terminal of the given delegate reads in a delegation server information on the delegates and the titleholders of the group thus constituted. The data and the information read and a private key of the given delegate are applied to a cryptographic algorithm to produce a signature which therefore carries a cryptographic delegation mark. The data, information, and signature are transmitted to a user terminal that can trace the characteristics of the signature delegation.